NICE Actimize

CELENT

Report

AI VS. DIRTY MONEY

State of Artificial Intelligence in Financial Crime Compliance

July 10, 2024

Ian Watson

David Choi

This report was commissioned by NICE Actimize, which asked Celent to design and execute a Celent study on its behalf. The analysis and conclusions are Celent's alone, and NICE Actimize had no editorial control over report contents.

CELENT

AI VS. DIRTY MONEY

State of Artificial Intelligence in Financial Crime Compliance

Ian Watson
David Choi

July 15, 2024

This report was commissioned by NICE Actimize, which asked Celent to design and execute a Celent study on its behalf. The analysis and conclusions are Celent's alone, and NICE Actimize had no editorial control over report contents.

CONTENTS

NOW IS THE TIME FOR AI IN FINANCIAL CRIME COMPLIANCE

Last year, $3.5 trillion was laundered globally. Since 2014, that amount has grown at a compound annual growth rate (CAGR) of 5%[1]. Decades of work by banks and billions of dollars have gone into developing technology and operations for anti-money laundering, and this investment shows no sign of slowing. In 2023, banks in the United States filed 2 million suspicious activity reports (SARs), a 7% increase from 2022 and up 62% since 2020[2]. All this effort has built up financial crime compliance (FCC) units within financial services companies into technology and operations behemoths.

Traditionally banks have struggled with false positive rates of greater than 90%[3] and have had to add armies of investigators to keep pace with an ever-growing number of investigations. Financial Crime Compliance executives balance tight turnaround times with the risk of punishing fines for non-compliance and must continually update detection rules to fight increasingly sophisticated laundering techniques.

Enter artificial intelligence (AI). Already selectively implemented to help banks analyze the massive volumes of transactions they must assess, breakthroughs in machine learning (ML), including advancements in language capabilities underpinning GenAI, promise to drive down costs while improving effectiveness. New abilities to identify hidden patterns, synthesize structured and unstructured data, and explain analytical findings in a narrative are boosting investigator efficiency, detecting new types of laundering and flagging suspicious activity in real time. The increasing adoption of machine learning, including generative AI, is tipping the scales in the balance between regulatory compliance and effective financial crime compliance.

But where to start? AI is a broad term. There are forms of AI that have arguably been around since the 1950s, while the latest form, GenAI, is being touted as a panacea to any business problem you can think of. This paper is meant to help FCC executives make the most of this new, and not so new, technology.

[1] Celent estimate 2023

[2] Fincen SAR statistics

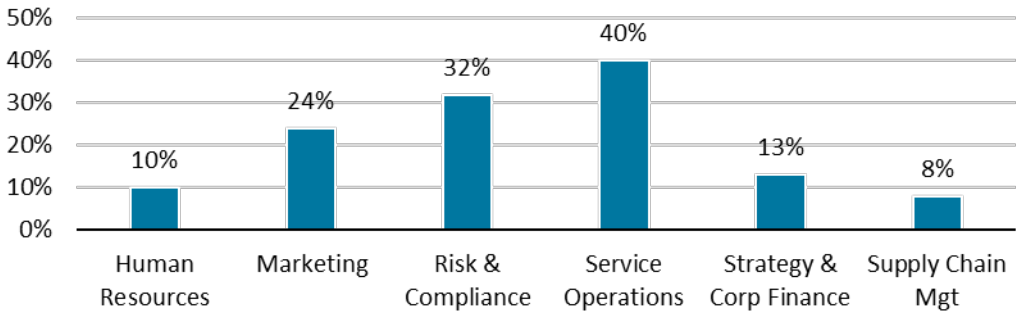
[3] *Changing the Rules: The Evolution of Transaction Monitoring, Celent, February 2023*

RISK AND FCC ARE AT VANGUARD OF AI ADOPTION

There is currently intense interest within the boardroom and C-Suite to apply GenAI to a broad variety of problems. Adoption of GenAI is proceeding rapidly with technology front runners already having GenAI use cases in production. This interest is creating fertile ground for investment in all types of AI, and we are seeing the Risk and Compliance function (and FCC within it) in the vanguard of adoption.

The financial services industry has the highest AI adoption rate[4] of all industries except for the high tech[5] industry. Within financial services, Risk and Compliance has the second highest AI adoption of all the business functions, behind only Service Operations (see Figure 1).

Figure 1: AI Adoption by Function in Financial Services



Source: 2022 AI Index Report, Human-Centered Artificial Intelligence, Stanford University

With pressure from the board and C-Suite to stay on the competitive edge of this technology, Risk and Compliance executives must make hard decisions about where banks will deploy limited AI resources to generate the most effective results. GenAI grabs the headlines in the media, as well as the attention of senior leadership, but it is not necessarily the technology that is going to produce the most consistent or impactful results. More established

[4] 2022 AI Index Report, Human Centered Artificial Intelligence, Stanford University

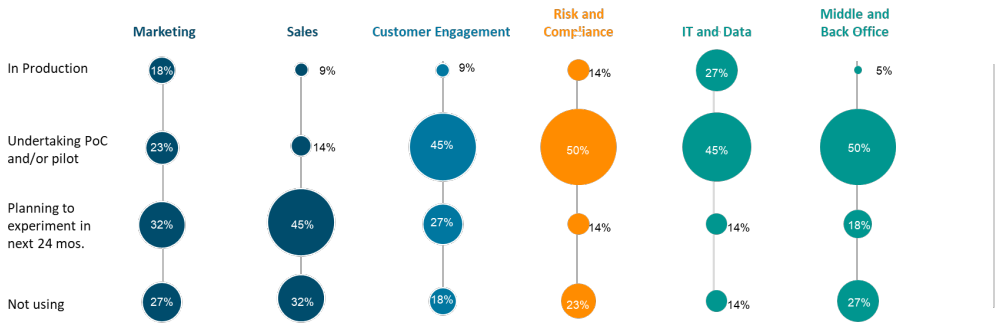
[5] Collection of computer systems and semiconductor manufacturers, software publishers, and data processing and hosting service providers

machine learning approaches have a track record of improving performance in transaction monitoring and sanctions screening with lower implementation risk.

In March 2024, Celent surveyed 23 bank executives in roles tied to innovation about the state of their adoption of GenAI across different areas within the bank. Survey participants tended to be innovation frontrunners and hence are ahead on the GenAI adoption curve compared to the majority of banks.

While we didn't ask about AML or sanctions specifically, we did see that the Risk and Compliance function was second only to the IT function when we look at the percentage of projects in either production or in proof of concept. Many of these are financial crime compliance use cases.

Figure 2: GenAI Adoption Rates by Function in Banking



Source: Celent Bank GenAI Adoption Survey March 2024

This survey further found that within Risk and Compliance, banks view detection models for AML and fraud as the leading high-impact use case for GenAI, as they look forward to how GenAI will improve on the pattern recognition and anomaly detection of traditional ML models. Information analysis (including summarization of flagged transactions) was the second-highest. There are other areas of financial crime compliance, like transaction monitoring, where there isn't a clear role for GenAI but other forms of AI are making a large impact.

WHERE AI IS USED IN FCC

There are three advanced AI technologies (see sidebar) that represent substantially improved capabilities beyond traditional rules-based systems: machine learning, deep learning, and generative AI. These build on each other but offer distinct differences in capability—they are good at different types of tasks.

Advanced AI Technologies

Machine Learning—Algorithms trained to make decisions by learning structures and patterns in data without being explicitly programmed on what to look for. ML supports predictive analytics and anomaly detection, as well as practical applications like computer vision, speech recognition, and language processing

Deep Learning—Algorithms inspired by the structure of the human brain. DL models like neural networks have proven to be highly effective in many generative tasks. They can recognize patterns and perform tasks such as image classification, speech recognition, and language translation.

Generative AI—An advanced form of deep learning, Gen AI uses algorithms to analyze data and learn patterns, enabling the creation of new, original content or designs, such as text, images, or music, often having been trained on vast datasets.

Machine learning's strength lies in its ability to continuously learn from new data. The models can autonomously adapt and improve their accuracy over time. They are also very good at handling complex and unstructured data. Deep learning excels at automatically learning hierarchical representations from large amounts of data. This allows it to find new patterns in data without being explicitly pointed at those patterns, e.g., finding new types of money laundering typologies. GenAI is a newer form of deep learning that can generate new content, such as images, text, or music, that resembles human-created content. Its strength is synthesizing unstructured data from internal systems and external searches to bring relevant data sets together, then making an initial determination for a human analyst to review.

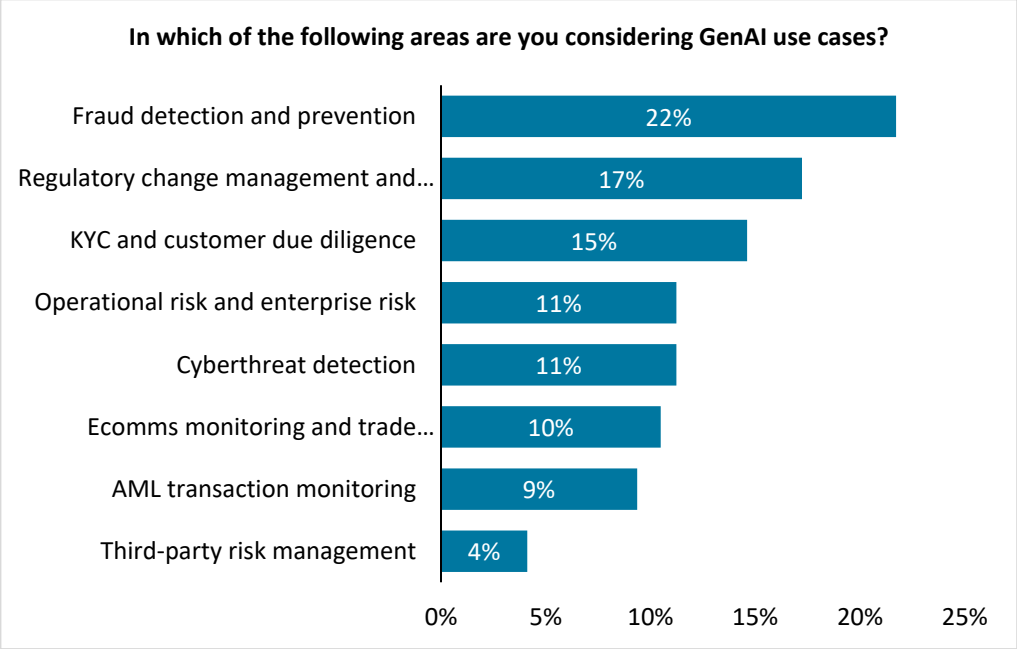
These three technologies are also at different stages of adoption and proven effectiveness. Machine learning is the most widely adopted and has proven its impact. Deep learning is next and GenAI is just at the beginning of the adoption cycle. As a result, the FCC use cases that provide the biggest impact may include not only GenAI but a combination of these AI technologies. Different models are good at different things, and it is often best to bring together their capabilities.

In March of 2024, Celent asked 200 risk leaders across North America, Europe, and Asia which areas within Risk and Compliance were they considering applying GenAI (see Figure 3). Combatting fraud

remains a paramount concern, as GenAI's data analysis and pattern recognition capabilities empower banks to proactively detect early signs of potentially fraudulent activities. Regulatory change management was second. GenAI and LLMs can be effective in cleaning up the tangle of duplicative policies across the bank and speeding up banks' compliance with new regulations.

Know-your-customer (KYC) was the third-most-popular use case. As we will discuss later, LLMs can play a role in synthesizing client data, documents, transactional history, and adverse media during client due diligence.

Figure 3: Application of GenAI within Risk and Compliance



Source: Celent 2024 Dimensions Survey—Risk

Transaction monitoring (TM) ranked lower as a priority for GenAI because banks see more promise in using predictive and anomaly detection machine

learning models to risk rate and triage alerts. To illustrate the differences in capability between these technologies, let's compare the priority use cases for GenAI with where these same executives believe that AI and ML are already having the biggest impact. In Figure 4, we see that TM, while a lower priority for GenAI, came out far ahead in terms of where AI is currently having the most impact. Thirty-eight percent (38%) of these executives said TM was where AI was having the most impact, versus 27% for fraud and 25% for KYC.

Societe Generale RegWatch Chatbot

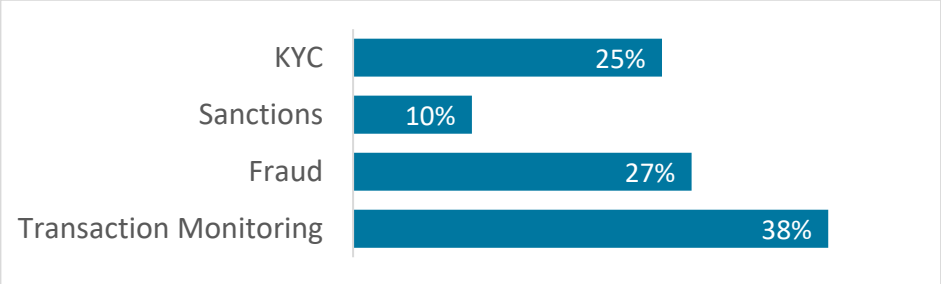
To help bank employees navigate the complexities of the regulatory landscape, Societe Generale's compliance group uses NLP and GenAI models packaged as a RegWatch app like a chatbot.

Trained on the corpus of internal policies and external regulations, the chatbot serves as a virtual compliance officer, answering general questions about internal policies or proposing content generation like a summary. It can advise business line teams on whether unit policies are up to date and also make them aware of new regulatory requirements and which policies need to be updated as a result.

It isn't surprising that transaction monitoring is so far ahead. AI and automation have been critical in allowing banks to monitor large volumes of customer transactions, and adding machine learning has made a dent in reducing false positives and improving true positives.

Many banks are focusing their AI efforts in transaction monitoring on machine learning, not GenAI, to combat false positives, drive down costs and detect new crime typologies.

Figure 4: Effectiveness of AI by FCC Function



Source: Celent Financial Crime Survey, 2023

KYC had 25% of respondents call it out as where AI was having the most impact on their financial crime operations. Machine learning is increasingly being used to improve and automate the document verification process.

While GenAI will eventually be used to more accurately extract relevant information from authentication documents, and automate analysis of adverse media within the KYC process, this is not a top priority use case for this technology. KYC was a third priority for executives when asked about where they intended to develop GenAI use cases.

Only 10% of respondents picked sanctions as the area where AI was already having the greatest impact. Some of the earliest watchlist screening and matching systems were installed in the 1990s. Updating them has not been a priority, and there is still a good deal of legacy technology in place. That said, banks are using machine learning to support the prioritization of potential matches against watchlists.

REAL LIFE AI USE CASES IN FCC

AI has been used to fight money laundering for decades and we have seen step changes in its effectiveness with the introduction of machine learning and deep learning technologies. However, the rate of AI adoption across financial crime compliance processes has not been uniform. There have been varying rates of adoption across transaction monitoring, KYC, sanctions and investigations.

Transaction Monitoring

Banks were early in applying rules-based systems and simple forms of supervised machine learning for transaction monitoring. These were game-changing in analyzing large volumes of customer transactions, but the high number of false positive alerts and large teams that are required to investigate these alerts are pushing banks to newer forms of AI to combat false positives and drive down costs.

> *AI and machine learning are promising but right now that technology is entirely focused on improving efficiency, we need to point it at making these models more effective.*
>
> *Global Head of Sanctions, Canadian D-SIB*[6]

So, while rules still have a role to play in behavior detection, they are now widely being augmented with machine learning to triage alerts. This is the most frequent pattern of adoption as banks take a hybrid approach with machine learning-based detection balanced by rules that act as a baseline screen to ensure no obvious suspicious activity is missed. A hybrid machine learning/rules-based approach is also being used to improve anomaly detection. This is a more adaptive approach to identification of additional, previously unknown money laundering activities and it allows banks to identify potential money laundering schemes that would not be detected by rules-based screens, which are built to look for known, well documented red flags. This hybrid approach may be viewed more favorably by regulators who

[6] Domestic Systemically Important Bank

have confidence in rules-based systems but recognize AI's ability to aid in fighting financial crime.

As firms become more adept at building and deploying machine learning models, we are seeing a few banks deploying transaction monitoring solutions entirely based on machine learning. Advanced models are allowing for more sophisticated algorithms to detect complex cases and are looking more comprehensively at monitoring and detection. The limitations of this approach are that it requires an extensive, clean corpus of data to train the models and a wholesale replacement of current TM systems.

Another emerging trend is the use of graph databases to model a bank's complex network of financial transactions and relationships across legal entities, like directors, and beneficiaries. In graph databases, nodes represent different entities (such as people or organizations) and edges represent transactions between these entities. By looking at relationships and patterns of interactions between different entities over time, graph analytics can identify hidden connections and money laundering patterns across multiple transactions, intricate networks, and non-financial indicators like connections between entities found on social media.

Know Your Customer (KYC)

Much of the application of more advanced AI in KYC has been to increase the operational efficiency of customer due diligence by automating data collection, analyzing the resulting client file, screening against watchlists or adverse media, and summarizing the client's KYC data, transactional history, and risk profile.

These use cases also can be made more powerful with the addition of GenAI. Banks are using a combination of graph databases and LLMs to summarize sources more thoroughly, better analyze the nature of any allegations, assess the credibility of the source, score the severity of an indicator, and then provide a narrative explanation for potential risks.

ABN AMRO Case Study

ABN AMRO deployed a next-generation KYC investigation tool for complex KYC investigations. The solution identifies and tracks underlying beneficial owners and their associations. It optimizes financial crime detection and investigation by graphically displaying identified networks in an interactive manner and by highlighting risks for investigators. Laying out these networks for investigators makes them more efficient in evaluating customer risk and performing due diligence.

> *We use RPA[7] for rote administrative activity, but we are exploring machine learning to improve the effectiveness of our screening [during customer due diligence]*
>
> *Divisional Head of Financial Economic Crime, European D-SIB*

Advanced AI is also being used to automate customer data monitoring where AI is used to detect changes in a customer's profile and determine whether that customer's risk profile has changed. Once a customer's baseline behavior is established, machine learning models can continuously monitor customer activities to identify deviations from the established patterns. This makes it feasible to monitor a customer's risk profile on an ongoing basis, and facilitates a move to perpetual KYC.

Sanctions

Sanctions is the financial crime compliance area least impacted by AI to date, but that is changing as more advanced AI techniques are proven out in other areas. Banks are using ML-based risk scoring to automatically adjudicate alerts and hits. One global bank we spoke to recently implemented a combination of ML models and algorithmic/ probabilistic matching to reduce false positives within their sanctions screening programs. Banks are also looking at using LLMs to extract entity names and relevant data from unstructured data sources like social media and filings and then with advanced entity resolution resolve and deduplicate ambiguities in historical customer profiles.

One sanctions executive we talked to told us that network analysis based on graph databases had allowed them to cope with the 50%-75% increase in alerts from multi-lateral sanctions against Russia. Contextual

Sanctions Case Study

One G-SIB is implementing contextual detection of suspicious actors using entity resolution, advanced machine learning models, and graph networks. This method is not watching for suspicious transactions but instead is looking for suspicious people by building a network around them and seeing who they are connected to and transacting with, what corporate registries they are on, and what they find in adverse media scans. The project has reduced alert volumes by 80% while increasing the volume of reports sent to law enforcement by 200%.

[7] Robotic process automation

detection of suspicious actors using a combination of advanced entity resolution, machine learning models, and graph networks helped them reduce alert volumes by 40%. Instead of just looking at payments individually, he said, "we are looking for suspicious people first, then figuring out which transactions to flag."

> *We are looking at nations adjacent to those formally on sanction lists—e.g. [using graph analytics to look] at transactions in Turkey and UAE to find payments intended to get to Iran*.
>
> Head of AML and Sanctions, US-based G-SIB[8]

Investigations

The financial crime compliance process culminates in investigations, but to date there has been relatively low adoption of AI for investigations. Much of the effort in increasing FCC efficiency has been put into using machine learning to reduce the number of false positive alerts that investigators need to review. Now LLMs and GenAI can make the investigations process itself more efficient, and many banks are exploring or actively deploying these use cases.

LLMs' ability to read and make sense of human language allows banks to automate much of the investigations process. LLMs are being used to:

- consolidate case information by automatically extracting findings and key data from the initial alerts
- supplement data from internal sources with searches of external sources
- provide explanations of detected financial crime typologies (in transaction monitoring) or entity risk (in KYC) for analysts to review and adjudicate
- write case summaries or suspicious activity report (SAR) narratives to file with regulators

A few technology vendors in the FCC space have already launched LLM-based analyst copilots into the market. We have seen this adopted in large banks in North America, and initial users report that such tools can reduce the time to

[8] Global Systemically Important Bank

file a SAR by up to 70%.[9] However, no matter how advanced these systems get, human intervention will always be necessary to validate and cross-check sources for information before filing SARs.

[9] NICE Actimize press release, Feb 2024

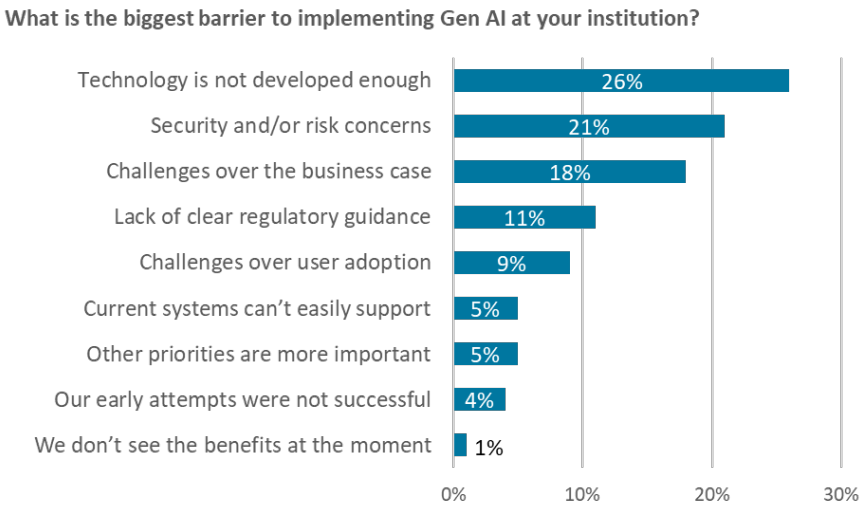
CONSIDERATIONS FOR IMPLEMENTATION

Financial Crime Compliance executives should use C-Suite enthusiasm about AI to bring forward proposals that use AI to reduce the cost and improve the effectiveness of FCC while also improving customer experience through fewer RFIs and fewer screened payments. However, once proposals are approved and even funded, barriers remain that FCC executives need to be aware of when implementing AI use cases in their organizations.

Pitfalls and Key Success Factors

In a recent Celent survey, we asked 600 financial services executives to rank the top three barriers they see to implementing GenAI. The majority of their top concerns were ones that will abate with time.

Figure 5: Barriers to Implementing GenAI



Source: Celent Dimensions Survey of 600 Financial Services executives, 2024

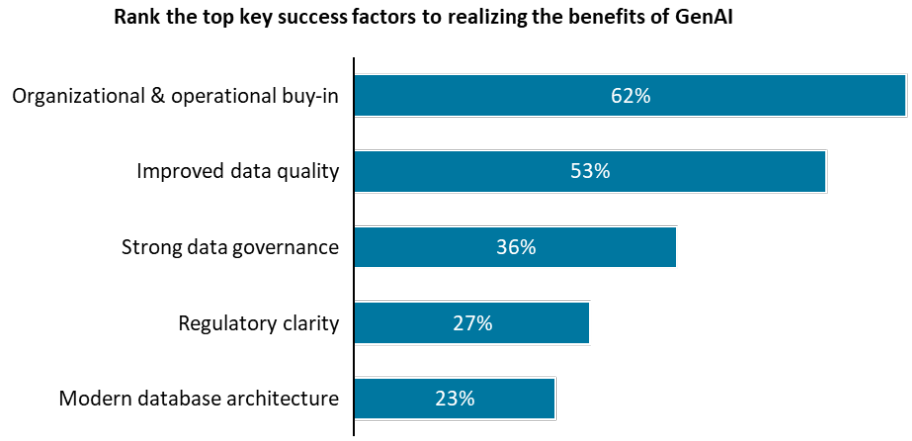
This is particularly true of the top concern, that "the technology is not developed enough." This was the top concern for 26% of respondents. This level of concern is specific to GenAI due to challenges in explainability,

transparency, and its most unique shortcoming, hallucinations.[10] However, GenAI technology is advancing rapidly with new approaches being built to address hallucinations, explainability and transparency.

The third and fourth concerns, "challenges over the business case" and "lack of clear regulatory guidance," will similarly recede as initial GenAI projects prove their benefits, and as regulators become comfortable with the technology as more and more banks move GenAI projects into production. Security will always be a concern, but it will be no greater than it is with other AI applications as technology groups gain more experience with GenAI.

So how best to overcome these issues? To get a view of what is working in GenAI, we surveyed 23 innovation leaders from banks who are currently deploying GenAI projects. We asked these executives, who all have roles tied to innovation, to rank 10 factors in order of which are most critical to success in deploying GenAI. Figure 6 shows the top five key success factors and the percentage of executives who ranked them as one of their top three key success factors.

Figure 6: Key Success Factors in Implementing GenAI Projects



Source: Celent Financial Services GenAI Adoption Survey March 2024

Two success factors were cited by more than half of the respondents: "organizational buy-in" and "improved data quality." Clients have consistently told us how critical good data foundations are in preparing for GenAI, but the fact so many are prioritizing buy-in is new. GenAI projects need greater emphasis on gaining buy-in due to their importance to senior leadership and

[10] Instances where a GenAI system makes up false information or facts that aren't based on real data or events creating outputs that are nonsensical or altogether inaccurate.

their broad interest in the organization, as well as the difficulty in calculating benefits and the unproven nature of their business cases.

"Regulatory clarity" was the third-most-critical success factor. This highlights the need to involve and inform regulators early in the process—particularly regarding projects rooted in financial crime compliance. The next two success factors (data governance and modern database architecture) are two other important parts of building a solid data foundation for AI.

Principles for AI Adoption

With these potential pitfalls and key success factors in mind, we recommend four principles for successful AI adoption in financial crime compliance.

1 Win over your stakeholders, INCLUDING… the external ones

Organizations must gain the buy-in of both internal and external stakeholders. Internally, capturing the innovative possibilities of requires strong collaboration between the business lines, the risk organization, and the compliance teams. The FCC team leading implementation should work closely with the following:

- model risk management to ensure the AI models meet standards
- business stakeholders for data and operational support
- technology to align on infrastructure and data requirements
- customer education to explain how you are governing AI to keep customers safe

In addition, financial crime compliance leaders should address internal "AI skeptics" via workshops and trainings and find "AI champions" to drive cultural adoption.

Externally, FCC leaders should be prepared to take regulators through their journey to demonstrate a careful risk-based approach and understand how regulators plan to utilize AI themselves. Many banks are waiting for another bank to be the first to implement, but providing regulators with clarity on the objectives and approach to applying AI can build the confidence to be the first to take that leap.

2 Get your data in order, AND… your data scientists

AI applications require enormous amounts of transaction, customer, and other bank data for initial training and ongoing functionality. But beyond quantity, the data must be of high quality—accurate, complete, consistent, and accessible. The higher the data quality, the more one can rely on the insights and findings an AI algorithm generates.

In a recent Celent survey, 27% of Risk and Compliance executives said that their number one technology priority was enhancing data quality and hygiene in order to boost AI readiness. This was the highest technology priority—above any other in the survey.

Break down silos in data science resources as well. One bank we talked to initially had 16 data and analytics teams across the business—none of whom had talked to each other until this year. They have since consolidated them into a cross-unit group that can serve different parts of the bank. Many banks already have chief data officers (CDOs). A recent survey of 116 Fortune 1000 companies found that 82.6% of them had a chief data officer. Of these, 48% considered data strategy as one of their primary responsibilities but only 16% said that analytics was.[11]

Some banks are expanding the CDO role into a CDAO (chief data and analytics officer) role. These individuals have a view of the breadth of a firm's AI investments. This role may not have control over all AI resources, but it is able to see all the investments being made and rationalize duplicative efforts. That said, there are different models depending on org structure, and a CDAO role won't make sense for many banks, but central funding, or the ability to centrally share capabilities and common components, is often an accelerator for deriving value from AI.

3 Make the case to innovate, BUT… stay focused on risk and regulation

While there is organizational urgency to move quickly on these high-profile projects, the FCC teams driving them must remain laser focused on effective management of risks, and delivery against regulatory obligations during the

[11] Data and Analytics Leadership Survey, New Vantage Partners, 2023

transition to AI. These projects have a high profile with regulators. In preparation, FCC and technology teams must clearly map and document how the AI solutions they are implementing mitigate financial crime risks and address regulatory requirements.

AI regulation is still in flux, as regulators balance the appeal of using this new technology to fight financial crime against a desire to maintain awareness and control over its potential risks, ethical implications, and the need for transparency and accountability in its application. Regulatory guidance will be clearer as formal frameworks for the responsible and effective use of AI are established and refined.

4 Strengthen AI Governance, AND… over-index on explainability

An Oliver Wyman survey of 23 UK high street banks[12] found that 95% already account for AI-related risks within their risk frameworks. Of these, 70% treat GenAI-related risks differently from the risks of traditional AI, and 65% of UK high street banks have already upgraded risk management policies to account for generative AI. Albeit a small group, they are setting the pace for proactively incorporating emerging AI technologies into risk management.

With the advent of GenAI, there is greater responsibility for AI governance to ensure that AI's role in preventing financial crime is transparent and comprehensible, particularly to those without a technical background. The documentation of AI's application is not just a procedural step; it's a bridge connecting the complex world of AI with the practical concerns of compliance and risk management. Moreover, with the emergence of GenAI and its greater opacity, the importance of designing AI processes that can clearly articulate the rationale behind decisions becomes even more critical for fostering trust and understanding with business sponsors as well as regulators.

[12] The Impact of AI in Financial Services, UK Finance, Oliver Wyman, Nov 2023

WHAT'S AHEAD

Adoption of these more advanced AI technologies is underway. GenAI is still in its infancy, and machine learning and deep learning are in early adoption. As we move to larger scale deployment of these technologies, they will enable a more holistic change to banks' risk and compliance operations.

Looking at the medium-term horizon, AI will increasingly address the fact that financial crime compliance processes in banks are fragmented. One executive we spoke to saw this fragmentation as the biggest barrier to more effectively preventing financial crime: "We are all missing stuff because of a lack of integration with the other financial crimes programs. One program with single point of accountability: That is the model that works."

Deployment of AI across FCC processes will allow banks to break down the silos between the client profile that is created during the onboarding process, the network analysis and adverse media analyses that they perform in watchlist screening for sanctions and PEPs, and the ongoing monitoring of transaction data. Going forward, we will see steady movement away from analyzing a customer's risk profile in slices. Instead, AI will allow banks to move to a continually updated, integrated view of their customers.

The adoption and integration of advanced AI technologies in Risk and Compliance is a transformative trend that's just beginning. As these technologies mature and scale, they will not only enhance the effectiveness of FCC processes but also redefine the landscape of financial risk management.

.

LEVERAGING CELENT'S EXPERTISE

If you found this report valuable, you might consider engaging with Celent for custom analysis and research. Our collective experience and the knowledge we gained while working on this report can help you streamline the creation, refinement, or execution of your strategies.

Support for Financial Institutions

Typical projects we support include:

Vendor short listing and selection. We perform discovery specific to you and your business to better understand your unique needs. We then create and administer a custom RFI to selected vendors to assist you in making rapid and accurate vendor choices.

Business practice evaluations. We spend time evaluating your business processes and requirements. Based on our knowledge of the market, we identify potential process or technology constraints and provide clear insights that will help you implement industry best practices.

IT and business strategy creation. We collect perspectives from your executive team, your front-line business and IT staff, and your customers. We then analyze your current position, institutional capabilities, and technology against your goals. If necessary, we help you reformulate your technology and business plans to address short-term and long-term needs.

Support for Vendors

We provide services that help you refine your product and service offerings. Examples include:

Product and service strategy evaluation. We help you assess your market position in terms of functionality, technology, and services. Our strategy workshops will help you target the right customers and map your offerings to their needs.

Market messaging and collateral review. Based on our extensive experience with your potential clients, we assess your marketing and sales materials—including your website and any collateral.

RELATED CELENT RESEARCH

GenAI-oneers in Risk & Compliance: Cross-Sector Survey and Spotlights
June 2024

Dimensions: Risk & Compliance IT Pressures & Priorities 2024 Edition
May 2024

GenAI by the Numbers: Insights from Celent's GenAI-oneers Banker Survey
May 2024

US and EU Regulators' Response to the Generative AI Tsunami
March 2024

COPYRIGHT NOTICE

For more information, please contact info@celent.com or:

Ian Watson iwatson@celent.com
David Choi dchoi@oliverwyman.com

Americas

USA
99 High Street, 32nd Floor
Boston, MA 02110-2320

+1.617.424.3200

USA
1166 Avenue of the Americas
New York, NY 10036

+1.212.345.8000

USA
Four Embarcadero Center
Suite 1100
San Francisco, CA 94111

+1.415.743.7800

Brazil
Rua Arquiteto Olavo Redig
de Campos, 105
Edifício EZ Tower – Torre B – 26º andar
04711-904 – São Paulo

+55 11 3878 2000

EMEA

Switzerland
Tessinerplatz 5
Zurich 8027

+41.44.5533.333

France
1 Rue Euler
Paris 75008

+33 1 45 02 30 00

Italy
Galleria San Babila 4B
Milan 20122

+39.02.305.771

United Kingdom
55 Baker Street
London W1U 8EW

+44.20.7333.8333

Asia-Pacific

Japan
Midtown Tower 16F
9-7-1, Akasaka
Minato-ku, Tokyo 107-6216

+81.3.6871.7008

Hong Kong
Unit 04, 9th Floor
Central Plaza
18 Harbour Road
Wanchai

+852 2301 7500

Singapore
8 Marina View
Asia Square Tower 1
#09-07
Singapore 018960

+65 6510 9700